Docket No.: 200701924-2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	10/754,378
Applicants:	:	Bindu Rama Rao, et al.
Filed:	:	January 9, 2004
TC/A.U.	:	3685
Examiner:	:	Charles C. Agwumezie
Title	:	AUTHENTICATION OF NOTIFICATIONS RECEIVED IN AN ELECTRONIC DEVICE IN A MOBILE SERVICES NETWORK

APPEAL BRIEF

MS APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madame:

This brief, in compliance with 37 C.F.R. § 41.37, is in furtherance of the Notice of Appeal filed under 37 C.F.R. § 41.31 filed May 24, 2010.

This brief is accompanied by the fee set forth in 37 CFR § 41.20(b)(2), as described in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. §41.37:

I. Real Party In Interest

II. Related Appeals and Interferences

III. Status of Claims

IV. Status of Amendments

V. Summary of Claimed Subject Matter

VI. Grounds of Rejection to be Reviewed on Appeal

VII. Argument

VIII. Claims Appendix

IX. Evidence Appendix

X. Related Proceedings Appendix

The last page of this brief bears the attorney's signature.

I. REAL PARTY IN INTEREST

The real parties in interest for this appeal are:

A. The Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

II. RELATED APPEALS AND INTERFERANCES

Appellant submits that no related application is presently undergoing appeal or interference proceedings.

III. STATUS OF CLAIMS

A. Total Claims: 1, 2 and 4-40

B. Current Status of Claims:

1. Claims canceled: 3
2. Claims withdrawn: none
3. Claims pending: 1, 2 and 4-40
4. Claims allowed: none
5. Claims rejected: 1, 2 and 4-40
6. Claims objected to: none

C. Claims on Appeal: 1, 2 and 4-40

IV. STATUS OF AMENDMENTS

No claims have been amended, canceled or added subsequent to the Final Office Action of May 17, 2010.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Independent Claim 1

Independent claim 1 recites a method of updating mobile electronic devices (Fig. 1: 107), the method comprising:

informing a notification history server (Fig. 1: 131) of notifications sent by various senders of updates (Para. [0057], lines 3-4; Para. [0056], lines 5-6) to a mobile electronic device (Fig. 1: 107) the notification history server (Fig. 1: 131) keeping a record of all verified and unverified notifications (Table 1 column 4), the notification history server (Fig. 1: 131) being distinct from various senders of updates (Para. [0057], lines 3-4; Para. [0056], lines 5-6) and distinct from a device management server (Fig. 1: 109) managing the mobile electronic device (Fig. 1: 107);

receiving a notification in the mobile electronic device (Fig. 1: 107); that an update is available from a particular sender (Para. [0056], lines 6-7);

determining authorization of the received notification (Para. [0058], lines 3-6) in the mobile electronic device (Fig. 1: 107) by sending, by the mobile electronic device (Fig. 1: 107), information retrieved from the received notification (Para.

[0059], lines 1-2) to the notification history server (Fig. 1: 131), and determining, by comparison (Para. [0059], lines 1-2) , whether the notification history server (Fig. 1: 131) has previously verified or unverified records of the notification (Para. [0059], lines 2-4; Para. [0059], lines 6-9) from the particular sender using the information sent by the electronic device (Fig. 1: 107) thereby avoiding testing and notification (Para. [0059], lines 8-9);

the mobile electronic device (Fig. 1: 107) downloading the available update from the particular sender (Para. [0059], line 5) if the notification history server (Fig. 1: 131) confirms having the verified record of notification (Para. [0059], line 4) from the particular sender of the notification; and

the mobile electronic device (Fig. 1: 107) ignoring the available update (Para. [0059], lines 8-9) from the particular sender if the notification history server (Fig. 1: 131) confirms having an unverified record of the notification (Para. [0059], lines 6-8) from the particular sender of the notification.

1. Claim 2 depends from independent claim 1 and recites that the method comprises simultaneously informing the notification history server (Fig. 1: 131) that the notification has been sent to the electronic device (Fig. 1: 107).

2. Claim 4 depends from independent claim 1 and recites that the method comprises ignoring the notification (Para. [0083], lines 4-6) in the electronic device (Fig. 1: 107) upon determining the notification is unverified (Para. [0059], lines 6-8);

recording that an unverified notification has been received (Para. [0083], lines 6-7); and

waiting to receive another notification (Para. [0083], ln. 7; Para. [0082], lines 1-2) in the electronic device (Fig. 1: 107).

3. Claim 5 depends from independent claim 1 and recites that the method comprises determining identification information of a server (Para. [0061], lines 1-2) and update package associated with the notification (Para. [0061], lines 5-6) upon determining that the notification received in the electronic device (Fig. 1: 107) is verified (Para. [0061], lines 4-5; Para. [0063], line 6, Para. [0065], lines 1-2).

4. Claim 6 depends from dependent claim 5 and recites that the method comprises retrieving the update package (Para. [0084], line 2; Para. [0085], lines 3-4);

and performing an update of at least one of firmware and software (Para. [0048], lines 5-6; Para. [0052], lines 7-8) in the electronic device (Fig. 1: 107).

5. Claim 7 depends from independent claim 1 and recites that the method of notification comprises one of a short message service (SMS) notification, an instant messaging (IM) notification, and an enhanced messaging service (EMS) notification (Para. [0089], lines 1-4; Para. [0060], line 2; Para. [0071], lines 1-6).

6. Claim 8 depends from independent claim 1 and recites wherein the electronic device (Fig. 1: 107) comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3, and a digital camera (Para. [0081], lines 3-5).

7. Claim 9 depends from independent claim 1 and recites wherein determining the authorization of the notification in the electronic device (Fig. 1: 107) comprises determining whether the notification was sent from an authorized server (Para. [0083], lines 3-5).

8. Claim 10 depends from dependent claim 9 and recites wherein an authorized server (Para. [0057], line 4; Para. [0083], lines 3-5) comprises one of a management server (Fig. 1: 109) and a customer care center (Fig. 1: 135).

9. Claim 11 depends from independent claim 1 and recites wherein notification comprises location and identification information (Para. [0084], line 4) regarding a management server (Fig. 1: 109) providing access to an update package (Para. [0051], lines 1-2; Para. [0084], line 3) and information regarding the update package (Para. [0084], line 6).

10. Claim 12 depends from dependent claim 11 and recites wherein location and identification information (Para. [0084], line 4) comprise at least one of a universal source locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol (Para. [0084], lines 7-9).

11. Claim 13 depends from independent claim 1 and recites that the method further comprises retrieving an update package (Para. [0084], line 3) from a default management server (Para. [0086], line 3) by accessing an address of the default management server when no server address information is included in the notification (Para. [0086], lines 1-3), the address of the default management

server being provisioned in the electronic device during a bootstrap provisioning event (Para. [0086], lines 3-5).

12. Claim 14 depends from claim 13, and recites wherein retrieving the update package (Para. [0084], line 3) from the default management server (Para. [0086], line 3) is performed after authorization of the notification message (Para. [0086], lines 7-8)

13. Claim 15 depends from independent claim 1, and recites that the method comprises retrieving an update package (Para. [0084], line 3) via a down agent (Fig. 1: 119) in the electronic device (Fig. 1: 107); and

updating at least one of firmware and software in the electronic device (Para. [0090], lines 6-7) via an update agent (Fig 1: 113) in the electronic device (Fig. 1: 107).

14. Claim 16 depends from independent claim 1, and recites that the method comprises preventing unauthorized updates of at least one of firmware and software (Para. [0096], lines 1-3) in the electronic device (Fig. 1: 107).

15. Claim 17 depends from independent claim 1, and recites the method wherein preventing unauthorized updates (Para. [0091], lines 3-4) comprises when a notification sent to the electronic device is discernable by an end-user (Para. [0093], line 2) and the end-user is prompted to initiate an update process (Para. [0094], line 1); and

when the end-user initiates the update process (Para. [0094], line 3), the electronic device is adapted to determine the authorization of the notification (Para. [0094], lines 3-5), and abort the update process if the notification

is determined to be unverified (Para. [0095], lines 3-4), and permit the update package to be downloaded, if the notification is determined to be verified (Para. [0095], lines 1-2).

16. Claim 18 depends from dependent claim 16, and recites that the method preventing unauthorized updates (Para. [0093], lines 3-4) comprises receiving a dynamic key component (Para. [0098], lines 1-2) from a management server in the electronic device;

accessing a static key component from memory (Para. [0098], lines 2-3) in the electronic device; and

instructing a download agent (Fig. 1: 119) to use the dynamic key component (Para. [0098], lines 1-2) and the static key component (Para. [0098], lines 2-3) to generate a security key (Para. [0098], lines 3-5), wherein the generated security key facilitates access to a downloadable update package (Para. [0098], line 6) in an update package repository (Fig. 1: 133) if the electronic device is authorized access to the update package, otherwise the electronic device (Fig. 1: 107) is denied access to the update package (Para. [0084], line 3).

17. Claim 19 depends from independent claim 1, and recites that the method comprises provisioning an address of a management server (Para. [0086], lines 3-4) in the electronic device (Fig. 1: 107) during a bootstrap provisioning event (Para. [0086], lines 3-4) by sending a notification (Para. [0086], lines 5-6). the notification comprising server address information (Para. [0085], lines 1-2), and wherein the electronic device (Fig. 1: 107) is adapted to access and employ the address of the management server (Para. [0086], lines 3-4) provisioned

in the electronic device (Fig. 1: 107) after the bootstrap provisioning event (Para. [0086], lines 3-4).

B. Independent Claim 20

Independent claim 1 recites a mobile services network (Fig. 1: 105) that comprises: at least one mobile electronic device (Fig. 1: 107);

a device management server (Fig. 1: 109) communicatively linked with the at least one mobile electronic device (Para. [0049], line 3) via a communication link (Fig. 1: 143) for managing at least one mobile device (Fig. 1: 107; and

a notification history server (Fig. 1: 131) distinct from the device management server (Fig 1: 109) and operatively connected to the management server (Fig 1: 109), the notification history server (Fig. 1: 131) comprising a record of all verified notifications and unverified notifications sent to the at least one mobile electronic device by various senders (Table 1, Para. [0063], lines 1-4), the various senders (Table 1 column 3) being distinct from the notification history server (Fig 1: 131), wherein the notification history server (Fig. 1: 131) is able to determine authorization of an available update (Para. [0061], lines 1-2) by comparing (Para. [0063], lines 5-6) whether the notification history server has previous verified or unverified records of notification (Table 1 column 4) from a particular sender (Table 1 column 3) thereby avoiding testing of each notification (Para. [0067], lines 5-7);

wherein the mobile electronic device (Fig 1:107) is adapted to:

receive notifications as to available updates to firmware on the mobile device (Para. [0048], lines 4-6);

send information retrieved from the notifications to the notification history server (Para. [0059], lines 1-2);

download available updates associated with notifications (Para. [0059], lines 3-5) sent to the notification history server for which the notification history server (Fig. 1: 131) has a previous verified record (Table 1 column 4; Para [0059], lines 4-5) from the particular sender (Table 1 column 3); and

ignore available updates associated with notifications to the notification history server for which the notification history server has a previous unverified record from the particular sender (Para. [0067], lines 6-8; Table 1 column 4).

1. Claim 21 depends from independent claim 20, and recites the network wherein the electronic device (Fig. 1: 131) at least comprises:

non-volatile memory (Fig. 1: 111);

a short message entity (Fig. 1: 127);

random access memory (Fig. 1: 125); and

security services (Fig. 1: 123) (Para. [0050], lines 1-3).

2. Claim 22 depends from dependent claim 21, and recites the network wherein the non-volatile memory (Fig. 1: 111) in the electronic device at least stores:

an update agent (Fig. 1: 113);

a firmware and real-time operating system (Fig. 1: 115);

an operating system layer (Fig. 1: 117);

a download agent or browser (Fig. 1: 119); and

an end-user related data and content (Fig. 1: 121) (Para. [0050], lines 1-4).

3. Claim 23 depends from independent claim 20, and recites the network wherein the electronic device comprises one of a mobile cellular phone

handset, personal digital assistant, pager, MP3 player, and a digital camera (Para. [0081], lines 3-5).

4. Claim 24 depends from independent claim 20, and recites the network wherein the electronic device (Fig. 1: 107) is adapted to receive notifications informing the electronic device (Fig. 1: 107) of availability of update packages at the management server (Para. [0080], lines 1-5).

5. Claim 25 depends from dependent claim 24, and recites the network wherein the notification history server (Fig. 1: 131) is adapted to determine whether a notification is authorized (Para. [0061], lines 1-5) by examining message identification information in the notifications (Para. [0066], lines 1-5).

6. Claim 26 depends from dependent claim 24, and recites the network wherein the electronic device (Fig. 1: 107) is adapted to download an update package from an update package repository (Fig. 1: 133) using an update agent (Para. [0088], lines 1-4) upon determining that a notification received in the electronic device is authorized authentic (Para. [0084], lines 1-2).

7. Claim 27 depends from dependent claim 24, and recites the network wherein the electronic device (Fig. 1: 107) is adapted to determine whether a notification originated from an authorized sender (Para. [0063], lines 4-6).

8. Claim 28 depends from dependent claim 27, and recites the network wherein an authorized sender (Para. [0083], line 2) is at least one of the management server (Fig. 1: 109) and a customer care center (Fig. 1: 135) resident in the network (Para. [0083], lines 1-4).

9. Claim 29 depends from independent claim 20, and recites the network comprising a short message center (SMC) (Fig. 1: 129) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server (Para. [0060], lines 1-2) or a customer care center (Fig. 1: 135), notifications to the electronic device regarding availability of update packages (Para. [0060], lines 3-4).

10. Claim 30 depends from independent claim 20, and recites the network according to claim 20 wherein notifications comprise at least one of a short message service (SMS) notification (Para. [0089], line 1), an instant messaging (IM)

notification (Para. [0089], line 2), an email notification (Para. [0089], line 2), a wireless application protocol (WAP) push message notification (Para. [0089], line 3), and an enhanced messaging service (EMS) notification (Para. [0071], lines 1-2).

11. Claim 31 depends from dependent claim 30, and recites the network wherein notifications comprise at least one user data field containing message identification information (Para. [0090], lines 2-3). .

12. Claim 32 depends from dependent claim 30 and recites the network wherein notifications comprise location and identification information (Para. [0084], line 4) regarding a management server (Fig. 1: 109) providing access to an update package and information regarding the update package (Para. [0084], lines 5-6). .

13. Claim 33 depends from dependent claim 32 and recites the network wherein location and identification information (Para. [0084], line 4) comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information (Para. [0084], line 7-9).

14. Claim 34 depends from independent claim 20 and recites the network wherein upon determining that a notification received in the electronic device is unverified (Para. [0067], line 7), the electronic device (Fig 1: 107) is adapted to ignore the notification and wait for another notification, and a record is created recording that an unverified notification has been received (Para. [0083], lines 4-7).

15. Claim 35 depends from independent claim 20 and recites the network wherein the management server comprises the notification history server and an update package repository (Para. [0083], lines 4-7).

16. Claim 36 depends from independent claim 20 and recites the network wherein the notification history server is incorporated into a short message center in the network (Para. [0073], lines 1-3). .

17. Claim 37 depends from independent claim 20 and recites that the network comprises a security service in the electronic device for preventing

unauthorized updating of at least one of firmware and software in the electronic device (Para. [0096], lines 1-3). .

18. Claim 38 depends from dependent claim 37 and recites the network wherein preventing unauthorized updates comprises:

when a notification sent to the electronic device (Fig. 1: 107) is discernable by an end-user and the end-user is prompted to initiate an update process (Para. [0090], lines 1-4). , and

when the end-user initiates the update process (Para. [0091], line 3), the electronic device is adapted to determine the authorization of the notification (Para. [0091], lines 3-4), and abort the update process if the notification is determined to be unverified (Para. [0091], lines 4-5), and permit the update package to be downloaded, if the notification is determined to be verified (Para. [0091], lines 5-7).

19. Claim 39 depends from dependent claim 37 and recites the network wherein preventing unauthorized updates comprises:

receiving a dynamic key component from a management server in the electronic device (Para. [0098], lines 1-2);

accessing a static key component from memory in the electronic device (Para. [0098], lines 2-3); and

instructing a download agent to use the dynamic key component and the static key component to generate a security key (Fig. 2: 240b; (Para. [0098], lines 3-4), wherein the generated security key facilitates access to a downloadable update package in an update package repository(Para. [0098], lines 4-7),, if the electronic device is authorized access to the update package (Para. [00100], lines 3-4), otherwise the electronic device is denied access to the update package (Para. [00100], lines 1-2).

20. Claim 40 depends from independent claim 20 and recites the network wherein the network is adapted to provision the address of the management server (Para. [0086], lines 3-4) in the electronic device (Fig. 1: 107) during a bootstrap provisioning event (Para. [0086], lines 3-4) by sending a notification (Para. [0086], lines 5-6). the notification comprising server address information

(Para. [0085], lines 1-2), and wherein the electronic device (Fig. 1: 107) is adapted to access and employ the address of the management server (Para. [0086], lines 3-4) provisioned in the electronic device (Fig. 1: 107) after the bootstrap provisioning event (Para. [0086], lines 3-4).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether or not claims 1, 2 and 4-40 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

B. Whether or not claim 26 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claimed the subject matter of the claimed invention.

C. Whether or not claims 1, 2 and 4-40 are unpatentable under 35 U.S.C. § 103(a) over Cheng et al (US Publication 2006/0282834) in view of Sadowsky (US Patent 6,123,737) and further in view of Peng (US Publication 2001/0052052).

VII. ARGUMENT

A. Applicant's specification describes and fully supports the subject matter of independent claim 1, and dependent claims 2, 4-19.

1. Applicant's specification describes and fully supports the subject matter of independent claim 1.

Appellant respectfully submits that Appellant's specification describes the subject matter of independent claim 1 and dependent claims 2, 4-19 in such a way as to reasonable convey to one skilled in the relevant art that the inventors, at the time the Application was filed, had possession of the claimed invention. Independent claim 1, recites in part:

> determining authorization of the received notification the mobile electronic device by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining, by comparison, whether the notification history server has previously verified or unverified records of the notification from the particular sender using the information sent by the electronic device, thereby avoiding testing

and notification.

The Applicant respectfully submits, contrary to the assertion made in the Final Office Action, that "the specification as originally filed contains no support for 'thereby avoiding testing of each notification'", the specification does have support for "thereby avoiding testing of each notification".

The support for independent claim 1 can be found various location in the specification. Para. [0059], lines 6-9 states "if the notification server is unable to confirm knowledge of the notification.... then the electronic device may ignore the received notification and continue processing". Applicant contends that "thereby avoiding testing of each notification" is clearly supported by the language "ignore.. and continue processing", and therefore is fully described and supported by the specification.

Further support for "thereby avoiding testing of each notification" can be found at Para. [0083], lines 3-4, and Para. [0095], lines 3-4 Applicant submits that "thereby avoiding testing of each notification" is clearly supported by the specification language. Applicant points specifically to the language of Para. [0095], lines 1-4 where the language states "if the notification is found to be authentic, the electronic device may retrieve the update/modification package 260a and perform the update or modification. However, if the notification is determined to be inauthentic or unverified, the download procedure is aborted 280a and the notification is ignored."

The Applicant respectfully submits, the specification has support for

"thereby avoiding testing of each notification". Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 112, first paragraph, rejection of independent claim 1.

2. Applicant's specification describes and fully supports the subject matter of dependent claims 2, 4-19.

Dependent claims 2, 4-19, which depend from independent claim 1, are not argued separately for purposes of appeal from the arguments present above for independent claim 1. That is, Applicant respectfully submits that the applicant's specification describes and fully supports the subject matter of independent claim 1. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 112, first paragraph, rejection of dependent claims 2, 4-19, which depend from independent claim 1.

3. Applicant's specification describes and fully supports the subject matter of independent claim 20.

Applicant presumes the Examiner found claim 20 lacked support in the same manner as claim 1, such that "the specification as originally filed contains no support for 'thereby avoiding testing of each notification'". Claim 20 is not argued separately for purposes of appeal from the arguments present above for independent claim 1. That is, Applicant respectfully submits that the applicant's specification describes and fully supports the subject matter of independent claim 20, including "thereby avoiding testing of each notification". Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 112, first paragraph, rejection of

independent claim20.

4. Applicant's specification describes and fully supports the subject matter of dependent claims 21-40.

Dependent claims 21-40, which depend from independent claim 20, are not argued separately for purposes of appeal from the arguments present above for independent claim 20. That is, Applicant respectfully submits that the applicant's specification describes and fully supports the subject matter of independent claim 20. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 112, first paragraph, rejection of dependent claims 21-40, which depend from independent claim 20.

B. Applicant's claim 26 language is not indefinite and does particularly point out and distinctly claim the subject matter of dependent claim 26.

Applicant respectfully submits that Applicant's claim 26 language is not indefinite and does particularly point out and distinctly claim the subject matter of dependent claim 26. Independent claim 26, recites in part, "upon determining that a notification received in the electronic device is authorized authentic". Applicant respectfully submits that one of ordinary skill in the art would appreciate that the language of claim 26 should be construed as authorized. Similar to claim 25 which was amended to recite "authorized" from the originally filed "authentic", one of ordinary skill in the art would appreciate the meaning to be authorized.

C. The Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of

Appellant's claims 1-2, and 4-40

1. The Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's independent claim 1.

Cheng, Sadowsky, and Peng, alone or in combination, fail to teach, determining authorization of the notification received in the mobile electronic device by "determining, by comparison, whether the notification has previous verified or unverified records of the notification from a particular sender using the information sent by the electronic device, thereby avoiding testing of each notification and the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification"... as recited in Appellant's independent claim 1.

Pages 4-5 of the Final Office Action dated February 25, 2010, states:

> Cheng does not explicitly teach determining authorization of the received notification in the mobile electronic device, by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining by comparison whether the notification history server has previous verified or unverified records of the notification from a particular sender using information sent by the electronic device thereby testing of each notification, and
>
> the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification.

Pages 5 of the Final Office Action dated February 25, 2010, refers to the Sadowsky reference (Figs. 3 and 4; Column 4, lines 40-50) and Peng reference (Para. [0061]) as addressing these elements.

Sadowsky discloses, "if a push notification is not present, processing is terminated at step 83... If a push notification is present, control passes to step 84." (Column 4, lines 41-53), also referred to as the "trigger" (Fig. 3) with no mention of comparing whether the notification history server has *previous verified or unverified*

records of the notification, and ignoring the available update with an unverified record. Sadowsky also discloses, "if the package is found to be non-authentic, processing is terminated at step 85".

Peng discloses, "the mobile device receives a notification from a gateway 108. Whether the original application is stored in the local cache is determined (step 704) . If not the notification is ignored (step 706)." (Para. [0060], lines 4-7) with no mention of comparing whether the notification history server has *previous verified or unverified records of the notification*, and ignoring the available update with an unverified record.

Sadowsky, Peng, and Cheng, alone or in combination, fail to teach:

> determining authorization of the received notification in the mobile electronic device by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining, by comparison, whether the notification has previous verified or unverified records of the notification from a particular sender using the information sent by the electronic device, thereby avoiding testing of each notification, and
>
> the mobile electronic device downloading the available update from the particular sender if the notification history server confirms having the verified record of notification from the particular sender of the notification; and
>
> the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification.

as provided, in part, in Applicant's claim 1.

As such, the reference do not teach or suggest each and every element of independent claim 1. Accordingly, Appellant respectfully requests reconsideration and withdrawal of the § 103(a) rejection of independent claim 1, as well as those claims that depend therefrom.

2. The Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's independent claim 20.

Applicant's argument for independent claim 20 follows identically to independent claim 1. Cheng, Sadowsky, and Peng, alone or in combination, fail to teach, determining authorization of the notification received in the mobile electronic device by

> the notification history server comprising a record of all verified notifications and unverified notifications sent to the at lease one mobile electronic device by various senders, the various senders being distinct from the notification history server, wherein the notification history server is able to determine authorization of an available update by comparing whether the notification history server has previous verified or unverified records of notification from a particular sender thereby avoiding testing of each notification

... as recited, in part, in Appellant's independent claim 20.

Pages 4-5 of the Final Office Action dated February 25, 2010, states:

> Cheng does not explicitly teach determining authorization of the received notification in the mobile electronic device, by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining by comparison whether the notification history server has previous verified or unverified records of the notification from a particular sender using information sent by the electronic device thereby testing of each notification, and
>
> the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification.

Pages 5 of the Final Office Action dated February 25, 2010, refers to the Sadowsky reference (Figs. 3 and 4; Column 4, lines 40-50) and Peng reference (Para. [0061]) as addressing these elements.

Sadowsky discloses, "if a push notification is not present, processing is terminated at step 83... If a push notification is present, control passes to step 84." (Column 4, lines 41-53), also referred to as the "trigger" (Fig. 3) with no mention of comparing whether the notification history server has *previous verified or unverified records of the notification*, and ignoring available updates associated with a

previous unverified record. Sadowsky also discloses, "if the package is found to be non-authentic, processing is terminated at step 85".

Peng discloses, "the mobile device receives a notification from a gateway 108. Whether the original application is stored in the local cache is determined (step 704) . If not the notification is ignored (step 706)." (Para. [0060], lines 4-7) with no mention of comparing whether the notification history server has *previous verified or unverified records of the notification*, and ignoring available updates associated with a previous unverified record.

Sadowsky, Peng, and Cheng, alone or in combination, fail to teach:

> the notification history server comprising a record of all verified notifications and unverified notifications sent to the at lease one mobile electronic device by various senders, the various senders being distinct from the notification history server, wherein the notification history server is able to determine authorization of an available update by comparing whether the notification history server has previous verified or unverified records of notification from a particular sender thereby avoiding testing of each notification

as provided, in part, in Applicant's claim 20.

As such, the reference do not teach or suggest each and every element of independent claim 20. Accordingly, Appellant respectfully requests reconsideration and withdrawal of the § 103(a) rejection of independent claim 20, as well as those claims that depend therefrom.

3. The Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's dependent claims 2, 4-19.

Dependent claims 2, 4-19, which depend either directly or indirectly from independent claim 1, are not argued separately for purposes of appeal from the arguments present above for independent claim 1. That is, Applicant respectfully submits that Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's

independent claim 1. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 103(a) rejection of dependent claims 2, 4-19, which depend from independent claim 1.

4. The Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's dependent claims 21-40.

Dependent claims 21-40, which depend either directly or indirectly from independent claim 20, are not argued separately for purposes of appeal from the arguments present above for independent claim 20. That is, Applicant respectfully submits that Cheng, Sadowsky, and Peng references, alone or in combination do not teach, suggest, or render obvious each and every element of Appellant's independent claim 20. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the § 103(a) rejection of dependent claims 21-40 which depend from independent claim 20.

CONCLUSION

Appellant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner and/or members of the Board are invited to telephone Appellant's attorney Edward J. Brooks III at (612) 236-0120 to facilitate this appeal.

At any time during the pendency of this application, please charge any additional fees or credit overpayment to the Deposit Account No. 08-2025.

CERTIFICATE UNDER 37 C.F.R. §1.8:
The undersigned hereby certifies that this correspondence is being electronically filed with the United States Patent and Trademark Office on

July 9, 2010

Christy Pesta
Name

Signature

Bindu Rama Rao, et al.
Glenn Hamasaki, et al.

By their Representatives:
Brooks, Cameron & Huebsch, PLLC
1221 Nicollet Avenue, Suite 500
Minneapolis, MN 55403

Atty: Edward J. Brooks III
Reg. No.: 40,925

7/9/2010
Date:

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method of updating mobile electronic devices, the method comprising:

informing a notification history server of notifications sent by various senders of updates to a mobile electronic device, the notification history server keeping a record of all verified and unverified notifications, the notification history server being distinct from the various senders of updates and distinct from a device management server managing the mobile electronic device;

receiving a notification in the mobile electronic device that an update is available from a particular sender;

determining authorization of the received notification in the mobile electronic device by sending, by the mobile electronic device, information retrieved from the received notification to the notification history server, and determining, by comparison, whether the notification history server has previous verified or unverified records of the notification from the particular sender using the information sent by the electronic device thereby avoiding testing of each notification;

the mobile electronic device downloading the available update from the particular sender if the notification history server confirms having the verified record of notification from the particular sender of the notification; and

the mobile electronic device ignoring the available update from the particular sender if the notification history server confirms having an unverified record of the notification from the particular sender of the notification.

2. (Previously Presented) The method according to claim 1, further comprising:

simultaneously informing the notification history server that the notification has been sent to the electronic device.

3. (Cancelled).

4. (Previously Presented) The method according to claim 1, further comprising:

ignoring the notification in the electronic device upon determining that the notification is unverified;

recording that an unverified notification has been received; and

waiting to receive another notification in the electronic device.

5. (Previously Presented) The method according to claim 1, further comprising determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is verified.

6. (Original) The method according to claim 5, further comprising:

retrieving the update package; and

performing an update of at least one of firmware and software resident in the electronic device.

7. (Original) The method according to claim 1, wherein the notification comprises one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

8. (Original) The method according to claim 1, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera.

9. (Previously Presented) The method according to claim 1, wherein determining the authorization of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server.

10. (Original) The method according to claim 9, wherein an authorized server comprises one of a management server and a customer care center.

11. (Original) The method according to claim 1, wherein the notification comprises location and identification information regarding a management server providing access to an update package and information regarding the update package.

12. (Original) The method according to claim 11, wherein location and identification information comprise at least one of a universal resource locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

13. (Original) The method according to claim 1, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event.

14. (Previously Presented) The method according to claim 13, wherein retrieving the update package from the default management server is performed after authorization of the notification message.

15. (Original) The method according to claim 1, further comprising:

retrieving an update package via a download agent in the electronic device; and

updating at least one of firmware and software in the electronic device via an update agent in the electronic device.

16. (Original) The method according to claim 1, further comprising preventing unauthorized updates of at least one of firmware and software in the electronic device.

17. (Previously Presented) The method according to claim 16, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authorization of the notification, and abort the update process if the notification is determined to be unverified, and permit the update package to be downloaded, if the notification is determined to be verified.

18. (Original) The method according to claim 16, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

19. (Original) The method according to claim 1, further comprising provisioning an address of a management server in the electronic device during a bootstrap provisioning event by sending a notification. the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

20. (Previously Presented) A mobile services network at least comprising:

at least one mobile electronic device;

a device management server communicatively linked with the at least one mobile electronic device via a communication link for managing the at least one mobile device; and

a notification history server distinct from the device management server and operatively connected to the management server, the notification history server comprising a record of all verified notifications and unverified notifications sent to the at least one mobile electronic device by various senders, the various senders being distinct from the notification history server, wherein the notification history server is able to determine authorization of an available update by comparing whether the notification history server has previous verified or unverified records of notification from a particular sender thereby avoiding testing of each notification;

wherein the mobile electronic device is adapted to:

receive notifications as to available updates to firmware on the mobile device;

send information retrieved from the notifications to the notification history server;

download available updates associated with notifications sent to the notification history server for which the notification history server has a previous verified record from the particular sender; and

ignore available updates associated with notifications to the notification history server for which the notification history server has a previous unverified record from the particular sender.

21. (Original) The network according to claim 20, wherein the electronic device at least comprises:

non-volatile memory;

a short message entity;

random access memory; and

security services.

22. (Original) The network according to claim 21, wherein the non-volatile memory in the electronic device at least stores:

an update agent;

a firmware and real-time operating system;

an operating system layer;

a download agent or browser; and

an end-user related data and content.

23. (Original) The network according to claim 20, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

24. (Previously presented) The network according to claim 20, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server.

25. (Previously Presented) The network according to claim 24, wherein the notification history server is adapted to determine whether a notification is authorized by examining message identification information in the notifications.

26. (Previously Presented) The network according to claim 24, wherein the electronic device is adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authorized authentic.

27. (Original) The network according to claim 24, wherein the electronic device is adapted to determine whether a notification originated from an authorized sender.

28. (Original) The network according to claim 27, wherein an authorized sender is at least one of the management server and a customer care center resident in the network.

29. (Original) The network according to claim 20, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages.

30. (Original) The network according to claim 20, wherein notifications comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification.

31. (Original) The network according to claim 30, wherein notifications further comprise at least one user data field containing message identification information.

32. (Original) The network according to claim 30, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package.

33. (Original) The network according to claim 32, wherein location and identification information comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information.

34. (Previously Presented) The network according to claim 20, wherein upon determining that a notification received in the electronic device is unverified, the electronic device is adapted to ignore the notification and wait for another notification, and a record is created recording that an unverified notification has been received.

35. (Original) The network according to claim 20, wherein the management server comprises the notification history server and an update package repository.

36. (Original) The network according to claim 20, wherein the notification history server is incorporated into a short message center in the network.

37. (Original) The network according to claim 20, further comprising a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device.

38. (Previously Presented) The network according to claim 37, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and

when the end-user initiates the update process, the electronic device is adapted to determine the authorization of the notification, and abort the update process if the notification is determined to be unverified, and permit the update package to be downloaded, if the notification is determined to be verified.

39. (Original) The network according to claim 37, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

40. (Original) The network according to claim 20, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification. the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None